REMARKS/ARGUMENTS

Claim Amendments

The Applicant has not amended any claims. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-7 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1 and 3-7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Mamros et al. (hereinafter Mamros) US Patent Number 6,360,269 in view of Patel et al, IP Security Working Group, Internet Draft, Revised SA negotiation mode for ISAKMP/Oakley, Intel Corporation (hereinafter Patel). The Applicant respectfully traverses the rejection of these claims.

The Mamros reference appears to disclose a protected "keepalive" message that is transmitted by a local computer to a remote computer for keeping the connection between the computers alive when the communications link between the remote and local computers has been idle. Mamros discloses a protected ISAKMP/Oakley command sent to the remote computer wherein the local computer must receive a protected acknowledgment from the remote computer so that the local computer does not terminate the communications link.

The Patel reference appears to disclose, using the ISAKMP/OAKLEY key management protocol for authentication, security association negotiation and key management. The ISAKMP protocol defines two phases whereby, in Phase 1 security association and keying material is agreed on by peer authenticates to secure ISAKMP messages. Phase 2 is used to negotiate security association for security applications. (Abstract)

The Applicant respectfully directs the attention of the Examiner to amended claim1.

1. (Previously Presented) A method of sending encrypted streamed data over an IP network from a first node to a second node, the method comprising:

using Internet Key Exchange (IKE) Phase 1 negotiation to establish an IKE security association (SA) between the first and second nodes;

entering IKE Phase 2 to negotiate an IPSec SA for each transmission direction;

passing the IPSec SA data to streamed data applications associated with the streamed data;

encrypting the streamed data at the first node with a cipher using a shared secret forming part of said IPSec SA;

constructing IP datagrams containing the encrypted streamed data, the datagrams not including an IPSec header or headers; and

sending the IP datagrams from the first node to the second node. (emphasis added)

The Applicant's invention discloses a method and apparatus for encrypting VOIP transmissions. The invention uses IKE Phase 1 negotiations to establish an IKE security association (SA) between the first and second nodes and IKE Phase 2 to negotiate a pair of IEPSec SAs. The advantage of using IKE phase 2 is that the IKE phase 1 negotiation need only be done occasionally, with IKE phase 2 being carried out each time a new connection is required (Para. 37). As is well known in the art, Phase 1 IKE (main mode exchange) sets up a keying channel (ISAKMP SA) between the two gateways and Phase 2 IKE (quick mode exchange) sets up data channels (IPsec SAs). Since the VOIP transmissions are not subjected to a complete IPSec procedure, only the IKE component is used and the resulting packets do not include IPSec headers. In the case of VoIP the absence of IPSec headers reduces unnecessary overhead and headers are not needed because voice data can tolerate some replay.

As noted above, the Patel reference discloses using ISAKMP phase 1 and phase 2. ISAKMP is cited as teaching phase 1 negotiation to establish security association and phase 2 negotiations for each transmission direction. However, ISAKMP is a protocol within the IKE protocol. Even though ISAKMP is used for security and authentication purposes, the two phases of ISAKMP are not the same as the two phases of IKE. The Mamros and Patel references do not disclose using IKE (see the

attached memo, *The Internet Key Exchange (IKE)*, RFC 2409, "4. Introduction") phase 1 and IKE phase 2 negotiations and employing only the IKE component to negotiate IPSec SA data relevant to the encryption. (Page 6, last paragraph) Further, and most importantly, neither Mamros nor Patel disclose sending a datagram without IPSec headers. (Page 7, first full paragraph, (Para. 38)) This being the case, the Applicant respectfully requests the withdrawal of the rejection of claim 1.

Claims 3-4 depend from amended independent claim 1 and recite further limitations in combination with the novel elements of claim 1. Therefore, claims 3-4 contain the novel limitations of claim 1. Amended independent claim 5 is analogous to and contains limitations similar to the novel limitations of amended independent claim 1. Claims 6 and 7 depend from claim 5 and contain the same novel limitations. The Applicant respectfully requests the withdrawal of the rejection of claims 3-7.

Claim 2 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Mamros et al US 6,360,269 (hereinafter Mamros) in view of Patel et al. IP Security Working Group, Internet Draft, Intel Corporation (hereinafter Patel) and further in view of Rao, et al. US 6,757,823 (hereinafter Rao). The Applicant respectfully traverses the rejection of this claim.

The Rao reference appears to disclose a method for providing secure signaling connections for packet data network telephony calls (VOIP) using H.323 protocol. Though Rao appears to provide secure signaling connections for VOIP, Rao does not supply the missing elements of sending a datagram containing the VOIP payload without IPSec headers and using only the IKE component of IKE Phase 1 and Phase 2 negotiation between nodes. Further, claim 2 depends from amended independent claim 1 and contains the same novel limitations. This being the case, the Applicant respectfully requests the withdrawal of the rejection of claim 2.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

Sidney L. Weatherford

By Sidney L. Weatherford
Registration No. 45,602

Date: November 17, 2005

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-8656
sidney.weatherford@ericsson.com

Network Working Group
Request for Comments: 2409
Category: Standards Track

D. Harkins
D. Carrel
cisco Systems
November 1998

The Internet Key Exchange (IKE)

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Table Of Contents

1. Abstract

ISAKMP ([MSST98]) provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independant; that is, it is designed to support many different key exchanges.

Oakley ([Orm96]) describes a series of key exchanges-- called "modes"-- and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication).

SKEME ([SKEME]) describes a versatile key exchange technique which provides anonymity, repudiability, and quick key refreshment.

This document describes a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.

2. Discussion

This memo describes a hybrid protocol. The purpose is to negotiate, and provide authenticated keying material for, security associations in a protected manner.

Processes which implement this memo can be used for negotiating virtual private networks (VPNs) and also for providing a remote user from a remote site (whose IP address need not be known beforehand) access to a secure host or network.

Client negotiation is supported. Client mode is where the negotiating parties are not the endpoints for which security association negotiation is taking place. When used in client mode, the identities of the end parties remain hidden.

This does not implement the entire Oakley protocol, but only a subset necessary to satisfy its goals. It does not claim conformance or compliance with the entire Oakley protocol nor is it dependant in any way on the Oakley protocol.

Likewise, this does not implement the entire SKEME protocol, but only the method of public key encryption for authentication and its concept of fast re-keying using an exchange of nonces. This protocol is not dependant in any way on the SKEME protocol.

3. Terms and Definitions

3.1 Requirements Terminology

Keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT" and "MAY" that appear in this document are to be interpreted as described in [Bra97].

3.2 Notation

The following notation is used throughout this memo.

HDR is an ISAKMP header whose exchange type is the mode. When writen as HDR* it indicates payload encryption.

SA is an SA negotiation payload with one or more proposals. An initiator MAY provide multiple proposals for negotiation; a responder MUST reply with only one.

<P>_b indicates the body of payload <P>-- the ISAKMP generic vpayload is not included.

SAi_b is the entire body of the SA payload (minus the ISAKMP generic header)-- i.e. the DOI, situation, all proposals and all transforms offered by the Initiator.

CKY-I and CKY-R are the Initiator's cookie and the Responder's cookie, respectively, from the ISAKMP header.

g^xi and g^xr are the Diffie-Hellman ([DH]) public values of the initiator and responder respectively.

g^xy is the Diffie-Hellman shared secret.

KE is the key exchange payload which contains the public information exchanged in a Diffie-Hellman exchange. There is no particular encoding (e.g. a TLV) used for the data of a KE payload.

Nx is the nonce payload; x can be: i or r for the ISAKMP initiator and responder respectively.

IDx is the identification payload for "x". x can be: "ii" or "ir" for the ISAKMP initiator and responder respectively during phase one negotiation; or "ui" or "ur" for the user initiator and responder respectively during phase two. The ID payload format for the Internet DOI is defined in [Pip97].

SIG is the signature payload. The data to sign is exchange-specific.

CERT is the certificate payload.

HASH (and any derivitive such as HASH(2) or HASH_I) is the hash payload. The contents of the hash are specific to the authentication method.

prf(key, msg) is the keyed pseudo-random function-- often a keyed hash function-- used to generate a deterministic output that appears pseudo-random. prf's are used both for key derivations and for authentication (i.e. as a keyed MAC). (See [KBC96]).

SKEYID is a string derived from secret material known only to the active players in the exchange.

SKEYID_e is the keying material used by the ISAKMP SA to protect the confidentiality of its messages.

SKEYID_a is the keying material used by the ISAKMP SA to authenticate its messages.

SKEYID_d is the keying material used to derive keys for non-ISAKMP security associations.

<x>y indicates that "x" is encrypted with the key "y".

--> signifies "initiator to responder" communication (requests).

<-- signifies "responder to initiator" communication (replies).

| signifies concatenation of information-- e.g. X | Y is the concatentation of X with Y.

[x] indicates that x is optional.

Message encryption (when noted by a '*' after the ISAKMP header) MUST begin immediately after the ISAKMP header. When communication is protected, all payloads following the ISAKMP header MUST be encrypted. Encryption keys are generated from SKEYID_e in a manner that is defined for each algorithm.

3.3 Perfect Forward Secrecy

When used in the memo Perfect Forward Secrecy (PFS) refers to the notion that compromise of a single key will permit access to only data protected by a single key. For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.

Perfect Forward Secrecy for both keys and identities is provided in this protocol. (Sections 5.5 and 8).

3.4 Security Association

A security association (SA) is a set of policy and key(s) used to protect information. The ISAKMP SA is the shared policy and key(s) used by the negotiating peers in this protocol to protect their communication.

4. Introduction

Oakley and SKEME each define a method to establish an authenticated key exchange. This includes payloads construction, the information payloads carry, the order in which they are processed and how they are used.

While Oakley defines "modes", ISAKMP defines "phases". The relationship between the two is very straightforward and IKE presents different exchanges as modes which operate in one of two phases.

Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. This is called the

ISAKMP Security Association (SA). "Main Mode" and "Aggressive Mode" each accomplish a phase 1 exchange. "Main Mode" and "Aggressive Mode" MUST ONLY be used in phase 1.

Phase 2 is where Security Associations are negotiated on behalf of services such as IPsec or any other service which needs key material and/or parameter negotiation. "Quick Mode" accomplishes a phase 2 exchange. "Quick Mode" MUST ONLY be used in phase 2.

"New Group Mode" is not really a phase 1 or phase 2. It follows phase 1, but serves to establish a new group which can be used in future negotiations. "New Group Mode" MUST ONLY be used after phase 1.

The ISAKMP SA is bi-directional. That is, once established, either party may initiate Quick Mode, Informational, and New Group Mode Exchanges. Per the base ISAKMP document, the ISAKMP SA is identified by the Initiator's cookie followed by the Responder's cookie-- the role of each party in the phase 1 exchange dictates which cookie is the Initiator's. The cookie order established by the phase 1 exchange continues to identify the ISAKMP SA regardless of the direction the Quick Mode, Informational, or New Group exchange. In other words, the cookies MUST NOT swap places when the direction of the ISAKMP SA changes.

With the use of ISAKMP phases, an implementation can accomplish very fast keying when necessary. A single phase 1 negotiation may be used for more than one phase 2 negotiation. Additionally a single phase 2 negotiation can request multiple Security Associations. With these optimizations, an implementation can see less than one round trip per SA as well as less than one DH exponentiation per SA. "Main Mode" for phase 1 provides identity protection. When identity protection is not needed, "Aggressive Mode" can be used to reduce round trips even further. Developer hints for doing these optimizations are included below. It should also be noted that using public key encryption to authenticate an Aggressive Mode exchange will still provide identity protection.

This protocol does not define its own DOI per se. The ISAKMP SA, established in phase 1, MAY use the DOI and situation from a non-ISAKMP service (such as the IETF IPSec DOI [Pip97]). In this case an implementation MAY choose to restrict use of the ISAKMP SA for establishment of SAs for services of the same DOI. Alternately, an ISAKMP SA MAY be established with the value zero in both the DOI and situation (see [MSST98] for a description of these fields) and in this case implementations will be free to establish security services for any defined DOI using this ISAKMP SA. If a DOI of zero is used for establishment of a phase 1 SA, the syntax of the identity payloads used in phase 1 is that defined in [MSST98] and not from any DOI-- e.g. [Pip97]-- which may further expand the syntax and semantics of identities.

The following attributes are used by IKE and are negotiated as part of the ISAKMP Security Association. (These attributes pertain only to the ISAKMP Security Association and not to any Security Associations that ISAKMP may be negotiating on behalf of other services.)